INTERPOL

Combatting Cyber-enabled Financial Crimes in the era of Virtual Asset and Darknet Service Providers

June 2020

By INTERPOL, NTU and CFLW Cyber Strategies

INTERPOL | NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | CFLW Cyber Strategies

Table of Contents

1. Introduction

The invention of Bitcoin in 2009[1] heralded in a decade of innovation in financial technology (FinTech). This decade saw the development of alternative cryptocurrencies, the underlying blockchain as distributed ledger technologies, and new payment and financing methods. Collectively referred to as Virtual Assets (VAs) that can be exchanged for value in fiat currencies, they play a critical role in this new technology space. According to the Financial Action Task Force (FATF)[2], VA is defined as a digital representation of value that can be traded or transferred digitally and used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities and other financial assets covered by the FATF.

As a result, a vibrant FinTech industry has emerged, empowered by cyberspace and other new technologies, with numerous Virtual Asset Service Providers (VASPs) worldwide.

A VASP, according to FATF, is any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies;
- Trading between virtual assets.

Today, the traditional banking system is one of the payment facilitators or money transmitters[3] for VASPs where regulation permits. New payment methods offered by the VASPs, which disrupted the traditional "Trust Third Party" role of the banking industry, will undoubtedly facilitate trade and improve consumer experience, in particular by simplifying borderless transactions, improving inclusion and enabling micro-credit. On the other hand, these innovations offer various opportunities to support financial crimes[4], such as money laundering and terrorist financing [Fanusie 2018].

Less harm to citizen can be achieved through more prevention. This paper is driven by this strategy to increase policing measures toward more prevention. Disrupting online criminal services to make cyber-enabled financial crimes unattractive and unprofitable, rather than only prosecuting criminals. A traditional approach to disrupt crimes through financial measures has been proven effective in combating crimes that involve the trading and transferring of traditional financial assets. Cyber-enabled financial crimes, which created new manifestations of financial crimes, influenced by VAs and privacy-preserving technologies, would require a revolutionary and integral approach towards solutions. Since the FinTech space is a public-private ecosystem, solutions to combating the aforementioned crimes require the involvement of multiple stakeholders, including regulators, RegTech providers, banks, cryptocurrency

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2009, https://Bitcoin.org/Bitcoin.pdf
[2] FATF, Guidance for risk-based approach to virtual assets and virtual asset service providers, October 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
[3] https://en.wikipedia.org/wiki/Money_transmitter
[4] How can criminals misuse virtual assets? FATF, http://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

exchanges, tax authorities, immigration, financial intelligence units, and of course, law enforcement.

This paper analyses the cyber-enabled component of financial crimes, with a specific focus on darknet and cryptocurrencies. In particular, innovative payment solutions and anonymity-enhanced cryptocurrencies (AEC) are being exploited by new white-collar criminals to build a service-based dark industry within a virtual underground economy (dark web). Intrinsic properties of cryptocurrencies, namely the (pseudo-) anonymity and non-traceability, do not comply with the baseline anti-money laundering and anti-illegal flow controls such as transparency of value transfer. This paper identifies various worrying trends driven by the cyber-enabled component. These trends have been mapped out with the currently leading security measures that can serve as input for the risk-based approach of the various stakeholders to combat innovative financial crimes.

The leading approaches within the international law enforcement community are assessed to evaluate how they improve attribution in cybercrime, help de-anonymize AEC payments and help prevent money laundering and terrorist financing. As a result, challenges and recommendations are identified for law enforcement in the area of cyber-enabled financial crime.

Research approach

The research approach is based on an in-depth analysis of trends in cyber-enabled financial crimes that affect VASPs, including specific darknet-based financial service providers. Second, it analyses the approaches and control mechanisms of leading regulations and security measures.

The analysis is based on three sources of information:

(1) Dark Web Monitor[5] (DWM). It is a repository of dark web data collected since 2013. It includes more than 200,000 unique addresses of onion services, of which about 15,000 are active services, the others are offline. This is not exhaustive, but it is considered representative to understand the insights. For each onion service, HTML pages are downloaded up to depth level 2[6]. These services are tagged according to the INTERPOL Taxonomy on Dark Web and Virtual Assets[7], typically addressing Service Categories (like Market, Shop, Service Provider, etc.) and Abuse Types (like Financial Crime, Cybercrime, etc.).
(2) Blockchain incidents database.[8] It lists 110 cyber security incidents known to have affected different VASPs.
(3) Policy guidelines and reports from (inter)national organizations, NGO's and industry.

[5] Dark Web Monitor: https://dwm.pm
[6] Level 2 means that web crawler is trying to reach the content following the hyperlinks found in the first level (the main page) of a website.

[7] https://github.com/INTERPOL-Innovation-Centre/DW-VA-Taxonomy
[8] Blockchain Security Solutions platform: https://bcss.pm

An assessment is made for the leading regulations and security measures to combat aforementioned crimes, as proposed by FATF, the International Monetary Fund (IMF) and the United Nations Office on Drugs and Crime (UNODC) recommendations, regulations such as the fifth EU Anti-Money Laundering Directive (AMLD5), combined with existing capabilities of law enforcement.

Organization of this assessment report

Section 2 provides an overview of trends of the cyber-enabled component in financial crimes illustrated by specific use cases. The Section 3 addresses the leading regulations and safety measures. Based on these two inputs, a gap analysis with discussion is performed in Sections 4 and 5, respectively. In Section 6, the conclusions cover a series of recommendations for police chiefs on new law enforcement capabilities with focus on policy levels, innovation in technology and international cooperation.

2. Trends in cyber-enabled financial crimes

While focusing on financial crimes such as money laundering and terrorist financing, in many cases these financial crimes facilitate other crimes. The same mechanism is seen for darknet and cryptocurrencies. Many other crime areas are currently being supported by the darknet and cryptocurrencies ecosystem, such as drug trafficking, child sexual abuse, cybercrime and violent extremism.

Based on the analysis of different use cases, five trends have been identified. The trends are ranked from traditional to more recent manifestations of the cyber-enabled components in financial crimes:

(1) Trade in credentials of cards, new payment methods and cryptocurrencies
(2) Cryptocurrency payments to support illegal transactions
(3) Suspicious transactions on specific cryptocurrency addresses (hubs)
(4) Cyber-attacks on cryptocurrency exchanges and other VASPs
(5) Large scale manipulation within blockchain ecosystems

Each trend is described in detail below, with concrete examples collected from the three sources of information introduced in the research approach section.

Trend 1. Trade in credentials of cards, new payment methods and cryptocurrencies

Payment data trading, also known as carding, originated in the 1980s and is arguably one of the most traditional forms of cyber-enabled financial crime. Usually, these credentials from credit and debit cards, bank accounts and personal information are stolen, often as a result of a successful cyber-attack. Nevertheless, new manifestations of payment data trade, like private key shops, are observed as well.

Credits and debit cards

Carding[9] takes place on many different platforms such as markets, shops and forums. Research by Caneppele [2019] shows that global credit card fraud increased by a factor of 20 between 1993 and 2016, representing a loss of about USD 1 billion to nearly USD 25 billion, illustrated by Figure 1. According to Nilson[10], credit card companies managed to keep the losses below 7.2% throughout the period.

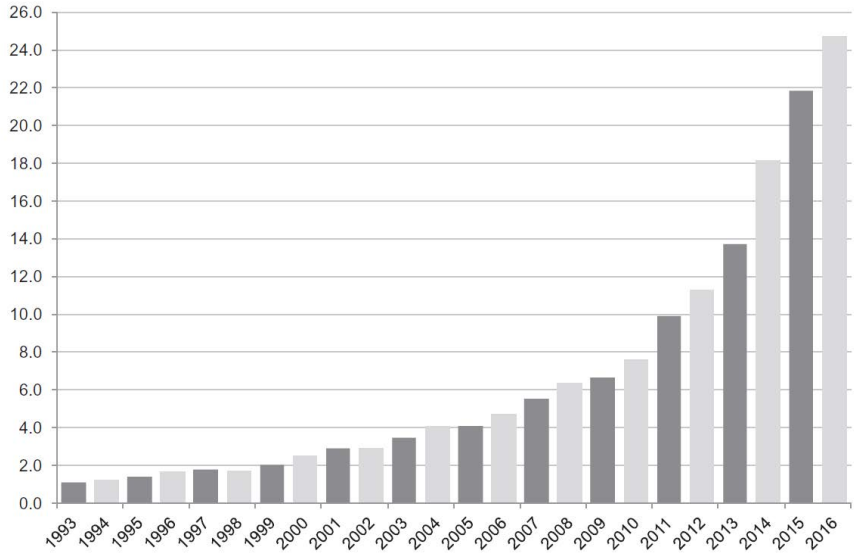


Figure 1. Card fraud worldwide (losses in billion dollars from 1993 until 2016)

Payment credential trading is one of the most active and prominent services offered on the dark web. Table 1 shows the percentages of active onion services within the dark web tagged by experts for different abuse types[11]. About 50% of the active services are tagged (7336 of 15,000 services). The different onion services have a wide variety of maturity levels: ranging from professional markets to services "under construction", or services offering redundancy with multi-mirror and duplicated onion services. This variety makes this dataset a representative sample to draw an understanding of proportion and nature of various crime areas in the dark web.

Table 1 shows that since 2013, a significant percentage of active services being monitored have supported financial crimes and sexual abuse. The abuse type "Financial Crime" is further divided into a series of subcategories as presented by Table 2. Onion services can be tagged with multiple subcategories, for example mixing services are mainly used to facilitate money laundering, and as such tagged for these subcategories. For this reason,

[9] Carding refers to frauds and trafficking related to stolen credit card details that are then used to create cloned cards or make online (so called "card-not-present") purchases.
[10] The Nilson Report (1068). Retrieved from https://www.nilsonreport.com/ (last accessed 3 December 2016). Nilson. (2016, October).
[11] Observed: 7 April 2020

the cumulative number of tags is larger than the total number of active financial crimes services.

Table 1. Absolute and relative number of active onion services tagged for Abuse Type

Abuse Type	Absolute number	Relative number
Financial crime	2982	42%
Sexual abuse	2658	36%
Drugs trade	768	10%
Violent crime	256	3%
Cybercrime	157	2%
Goods and Services	151	2%
Other	19	0%
No abuse	345	5%
Active and tagged onion services	**7336**	**100%**

Table 2 shows that carding has a substantial share of the financial crimes within the dark web. Furthermore, these figures show a substantial number of active mixing services and Ponzi schemes.

Table 2. Absolute and relative number of active onion services that facilitate financial crimes by different subcategories

Subcategory	Absolute number	Relative number
Carding	1707	57%
Money Laundering	707	24%
Mixing Service	526	18%
Ponzi Scheme	365	12%
Gambling	195	7%
Private Keys	23	1%
Match Fixing	12	0%
Financial crime (total)	**2982**	**100%**

Stolen credentials to operate through regulated payment providers

The analysis of search hits in DWM helped assess the presence and misuse of payment service providers within the dark web. One hit corresponds to one appearance of a search term within the DWM data repository. The number of hits is determined by the DWM search engine (similar to Google Search) and is counted for the name of a specific payment service provider. DWM contains an index of several million downloaded HTML pages from the dark web. This dataset is not exhaustive (the same way clear web search engines are also incomplete), but it is considered a representative set to assess the preference of payment providers whose stolen user credentials are for sale.

Table 3. Preference of different new payment methods in the dark web based on search hits for the payment method in DWM

Search term	Hits	Relative
PayPal	602.550	51%
Visa	222.646	19%
Western Union	158.496	14%
MoneyGram	68.416	6%
Mastercard	66.846	6%
American Express	24.283	2%
Moneybookers	12.135	1%
Maestro	11.569	1%
JCB	4.617	0%
Union Pay	729	0%
Diners Club	366	0%
Total	**1.172.653**	**100%**

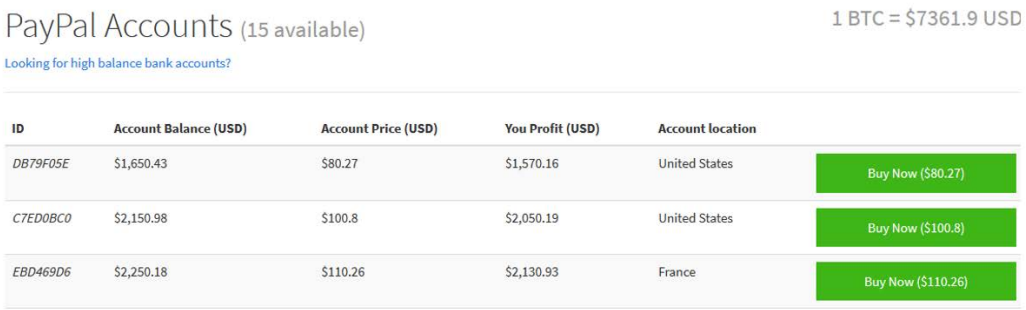
There is a percentage of cases where the context in which the names of this payment provider are found is unclear. Therefore, the numbers in the “Hit” column represent the sum of these underlying reasons. For example, the search term “PayPal” resulted in 602,550 hits, including PayPal login credentials and sites mentioning PayPal for other reasons. Table 3. shows the number of hits for the specific search terms such as “Visa”, “Western Union”, etc. as absolute number and relative[12] values. Table 3 provides insight into the demand for various payment methods within the dark web. Based on this dataset, PayPal is the number one payment method that appears on the dark web, followed by Visa and Western Union, which together make up over 80% of all hits.

A brief analysis of a random sample of about 100 onion services that contributed to the PayPal hits shows a dynamic trade in stolen credentials and hacked accounts in more than 90% of

[12] Observed: 2 April 2020

the cases. Figure 2 shows a screenshot of a shop that sells PayPal accounts. The first mention shows that a PayPal account is offered with an account balance of USD 1,650.43 and is selling for USD 80.27, which represents a huge incentive for the buyer. Assessing whether this is a scam or an account with a high risk of being caught is beyond the scope of this assessment. From the scraped data it is not possible to see whether there are any activities in these "for sale" accounts, further research is needed to explain the reasons for these observations and statistics. Regardless, the substantial presence of these shops on the dark web currently suggests that this business model of trading stolen credentials that exploit legitimate and regulated payment channels could benefit both sellers and buyers.

It is recommended to further analyse the exposure of these virtual asset and darknet service providers and derive inputs for a risk-based approach to interact with these organizations.


PayPal Accounts (15 available)

1 BTC = $7361.9 USD

Looking for high balance bank accounts?

ID	Account Balance (USD)	Account Price (USD)	You Profit (USD)	Account location	
DB79F05E	$1,650.43	$80.27	$1,570.16	United States	Buy Now ($80.27)
C7ED0BC0	$2,150.98	$100.8	$2,050.19	United States	Buy Now ($100.8)
EBD469D6	$2,250.18	$110.26	$2,130.93	France	Buy Now ($110.26)

Figure 2. PayPal accounts for sale by "TorVendor - Best PayPal & Bank Account Vendor on Tor"

Private key shops

Cryptocurrencies are a specific category within the FinTech innovation space. Since 2018, specific dark web shops have emerged that sell private keys of cryptocurrencies. Private keys are the most important credentials to enable cryptocurrency payments. Figure 3 shows an example of such a private key shop where clients can purchase private keys to unlock the assets available at a specific Bitcoin address. Usually, these keys are stolen during a cyber-attack on a cryptocurrency exchange, market or wallet provider. One way to clean up such accounts would be to set up a register of stolen credentials, where victims can claim their assets. This is a potential opportunity for law enforcement to work together with industry in order to develop such a register.

Table 2 shows the number of active private key shops (23), which is less common than, for example, carding shops (1707). However, it is important to realize that criminals will find new ways to sell their goods and constantly create new business models. In this case, the buyers of these private keys could shop to take advantage of the sale price and the market price. Their actions also enabled these buyers to poison blockchain analytics with patterns of mixing services. It is recommended for the community to keep scanning the horizon for new modus operandi within the space of darknet and cryptocurrencies, and to link activities for more synergistic insights to make less effort on false positives.

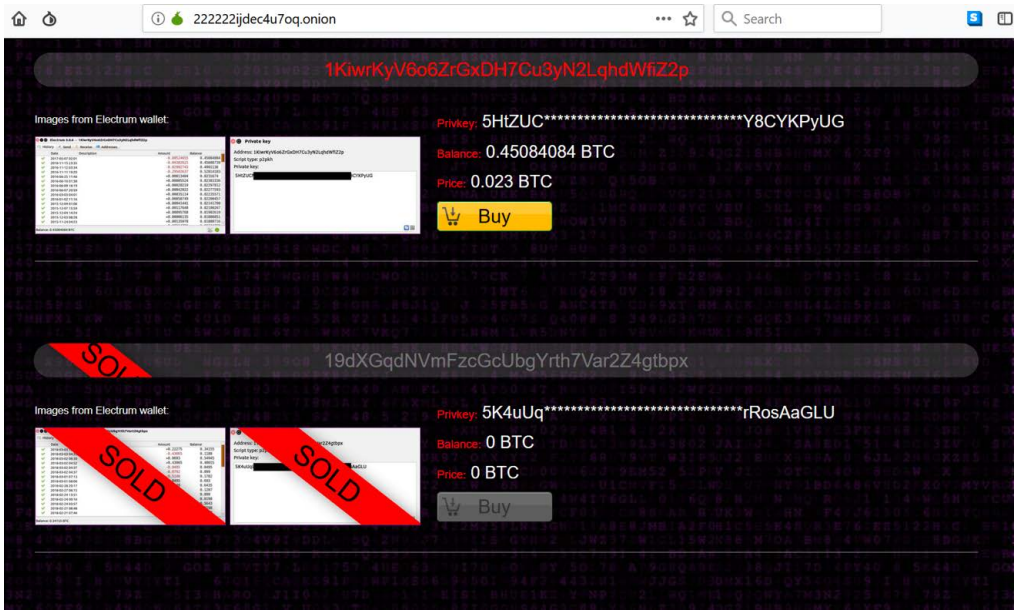


Figure 3. Screenshot of a Private Key Shop

Trend 2. Cryptocurrency payments to support illegal transactions

Suspicious transactions with cryptocurrencies are payments with cryptocurrencies for an illegal transaction, such as the purchase of illegal goods, the transaction paid in a ransomware or victims of sextortion, and money laundering transactions. One of the first significant illegal uses of Bitcoin was on Silk Road,[13] the first large-scale drug market within the dark web.

Cryptocurrency tagging

Since darknet and cryptocurrencies are involved in many crime areas, it is important to contextualize cryptocurrency addresses and payments by tagging these addresses with abuse type and service categories. Cyber security tools such as the DWM can be a relevant source of information, because every downloaded web page is analysed for the presence of cryptocurrency addresses. For example, Figure 3 presents two public Bitcoin addresses within the private key shop. Through this approach, DWM has collected nearly 1 million unique cryptocurrency addresses[14] since 2013. Using some clustering techniques as provided by blockchain analytics tooling these addresses can be used to contextualize even a fraction more addresses.

This information can be a starting point for an investigative attribution process. This investigation needs a combination of DWM and a blockchain transaction analysis tool like GraphSense to track transactions that end at a cryptocurrency exchange or wallet, with believed sufficient Know Your Customer (KYC) standards.

Figure 4 shows the statistics obtained from the DWM, showing that about 95% of the published addresses are Bitcoin, while Ethereum, Litecoin and Bitcoin Cash are limited. The liquidity of Bitcoin, due to the easiness to exchange for fiat currencies like USD, explains its dominance.

[13] https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
[14] Observed 7 April 2020.

Also, as long as customers are happy to use Bitcoin, criminals will continue accepting them. Further down the line, Bitcoin crime proceeds can always be traded for altcoins and StableCoins in highly active cryptocurrency markets such as Binance,[15] the largest cryptocurrency exchange market.

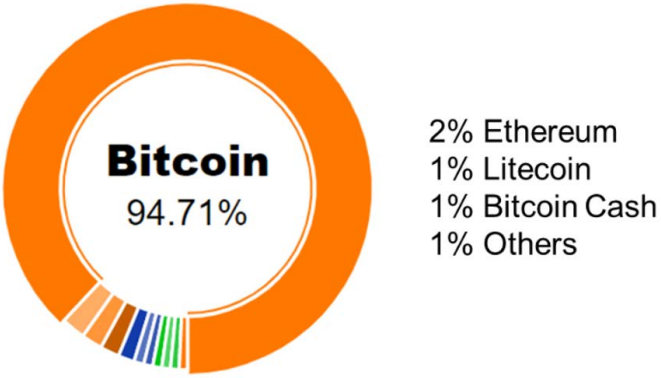


Figure 4. Distribution of published cryptocurrency addresses in the dark web, Bitcoin is still number one by far.

Blockchain analytics

During the INTERPOL Working Group on Darknet and Cryptocurrencies, altcoins,[16] and more specifically those considered AECs were identified as a priority challenge for policing. While Bitcoin is the most liquid cryptocurrency for payments to support criminal activity, users are less anonymous than they thought. That is why there is a demand for more anonymity. Additional research is needed to determine the proportions in which criminals prefer Bitcoin mixers over privacy coins (altcoins and AECs) to provide this additional level of anonymity. Experienced and better-skilled crypto criminals are known to value privacy protections by financial service providers. Therefore, it is desirable for law enforcement to be prepared for a stronger uptake of AECs and the use of advanced mixers.

Blockchain analytics tooling is an important capability that law enforcement agencies should use to track-and-trace suspicious transactions. Solutions are available such as Chainalysis,[17] Elliptic,[18] Coinbase,[19] MerkleScience,[20] Cointel[21] and many more. GraphSense[22] offers an advanced open source blockchain analysis tool. Most solutions are designed to cluster cryptocurrency addresses and contextualize these addresses with real-world identifiers to support investigations. In their 2020 Crypto Crime report[23], Chainalysis claims that about 1% of cryptocurrency transaction volume can be classified as illegal. Figure 5 illustrates this distribution for the period 2017-2019.

[15] Bitcoin Exchange | Cryptocurrency Exchange | Binance - https://www.binance.com/en
[16] https://www.interpol.int/en/News-and-Events/News/2018/Challenges-of-Altcoins-for-investigations-prosecutions-focus-of-INTERPOL-meeting
[17] https://www.chainalysis.com/
[18] https://www.elliptic.co/
[19] https://www.coinbase.com/
[20] https://merklescience.com/
[21] https://cointel.eu/
[22] https://graphsense.info
[23] The 2020 State of Crypto Crime - https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report

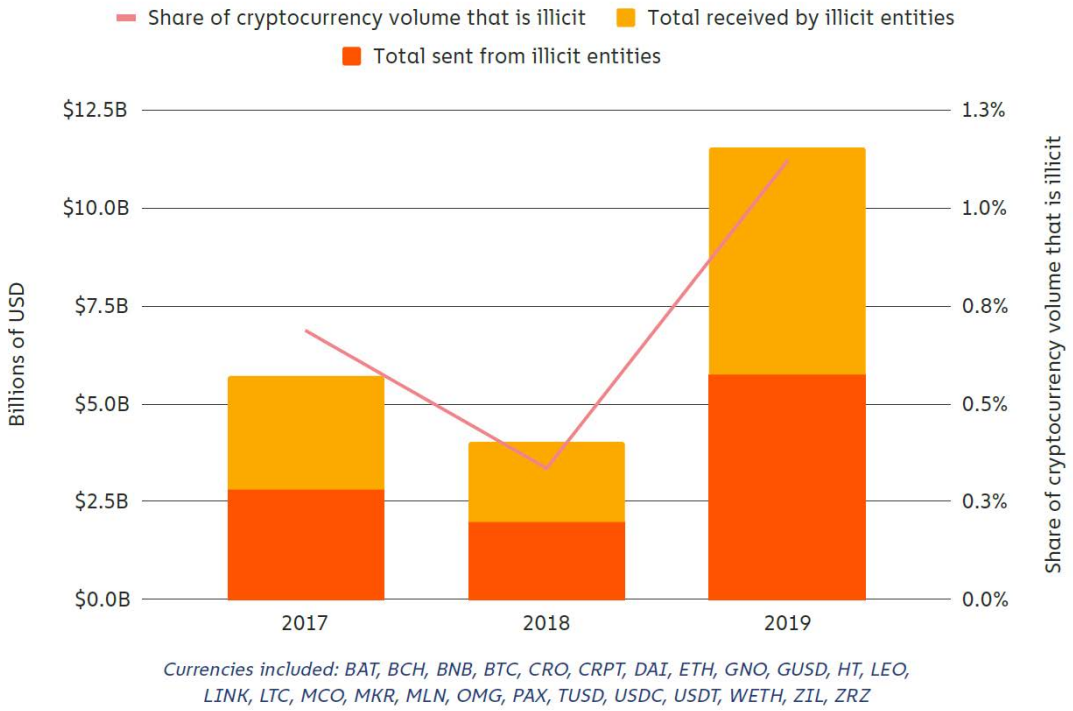


Figure 5. Total cryptocurrency sent and received by illicit entities vs illicit share of all cryptocurrency transaction volume, 2017 - 2019

Mixing services

Criminals are increasingly aware that the Bitcoin blockchain is pseudo-anonymous not anonymous. For this reason, they are making extra efforts to cover up the asset trail by using mixing services, sending contaminated cryptocurrencies to the mixers for it to be mixed "cleaner", uncorrelated transactions and wallets. Contaminated transactions or wallets are linked to criminal activities, they are also called tainted coins. Figure 6 provides a basic explanation of a mixing service as explained by McAfee.[24] It illustrates how these tainted "dirty" Bitcoins are processed and exchanged for "clean" Bitcoins. Clean Bitcoins cannot be attributed to criminogenic activities. The cleanest Bitcoins are the new Bitcoins generated by the Bitcoin mining process. This also illustrates the interest criminals have in the mining process. Mining will be discussed below.

[24] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/crypto-currency-laundering-service-bestmixer-io-taken-down-by-law-enforcement/

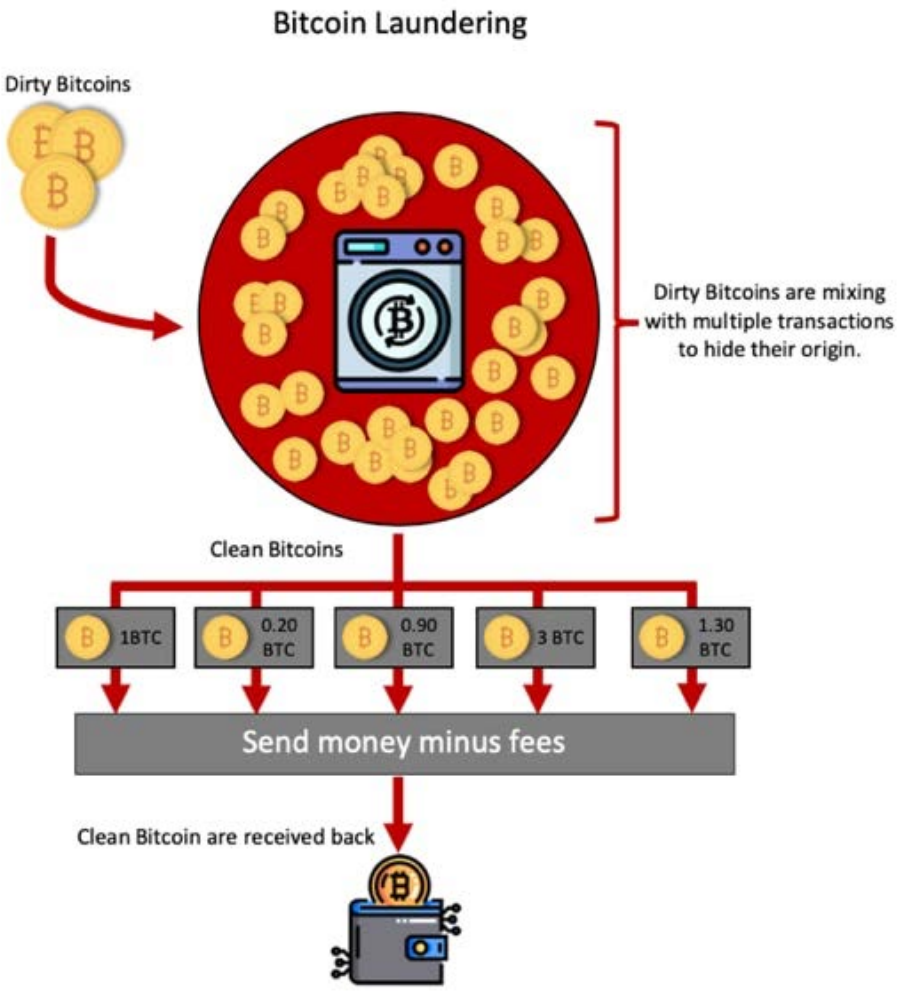


Figure 6. Basic explanation by McAfee of a mixing service. This was documented in a report after the takedown of bestmixer.io

DWM has identified 57 unique and active mixing services. The difference with the number of active mixing services (526) of Table 2 is explained by the large number of mirrors. These mirrors are now common cybersecurity practices by onion services in defence against DDoS attacks and law enforcement operations targeting darknet service providers. It requires new law enforcement cyber strategies to conduct takedown operations against these distributed service providers.

Trend 3. Suspicious transactions on specific cryptocurrency addresses

Cryptocurrency addresses with substantial activities, such as receiving over 1 million, can be considered suspicious hubs. This trend is illustrated by two cases where extreme numbers of transactions and Bitcoin value flow through these hubs.

Suspicious address

As a case study, one specific suspicious Bitcoin address amongst the almost 1 million extracted addresses in the DWM will be analysed in some detail. This address relates to a

Ponzi scheme that promised “100x Your Coins in 24 Hours”. This Bitcoin address has received over USD 900 billion in value, as can be seen in Figure 7. For a gambling service provider, this cannot be valid. Another explanation needs to be found through further analysis. It turned out that this particular address is the central Bitcoin address of a regulated cryptocurrency exchange. The question remains, why is this Bitcoin address advertised in a 100x benefits Ponzi scheme? The most likely explanation is that this central address has been intentionally and artificially associated within a Ponzi scheme by another entity. More research is needed to analyse the activities on this kind of hubs. It is recommended that law enforcement actively identify suspicious hubs, try to clarify the activity and monitor its behaviour. Tagging must be considered in policing but with caution, considering the source of the tag and the context to it.

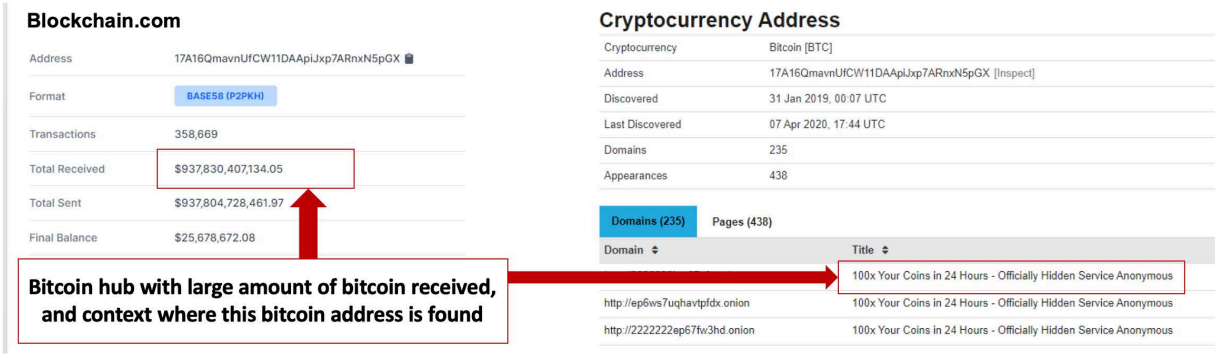


Figure 7. Suspicious activity through a specific Bitcoin address

Sextortion case

As shown in Table 1, a substantial share of active onion services are involved in sexual abuse services. According to recent research,[25] a new spam schedule has emerged since 2018: messages of sexual extortion that require payments in Bitcoin, also known as a sextortion campaign. This study analysed 4,340,736 sextortion spam emails to understand sextortion mechanisms. GraphSense blockchain analytics tooling made it possible to investigate the monetary flows between the actors involved to gain insight into the financial structure of these campaigns. Based on the 11-month study, it was found that a single entity controls the business operations and has revenues of approximately USD 1.3 million. This illustrates how lucrative sextortion with cryptocurrencies can be. The total revenue has been aggregated in about 50 cryptocurrency addresses. It is recommended for law enforcement to develop capabilities to analyse and improve attribution for those hubs.

Trend 4. Cyber-attacks on cryptocurrency exchanges and other VASPs

Many cyber-attacks on cryptocurrency exchanges and wallets have been reported since 2013. While cyber-attacks are not specific to financial crimes, financial institutions have always been one of the favourite targets for the majority of cyber criminals. In addition to stealing money or virtual assets, the credentials of hacked accounts are also relevant fruits of crime, making this an important trend to analyse.

[25] Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem, Masarah Paquet-Clouston, Matteo Romiti, Bernhard Haslhofer, Thomas Charvat, 2019

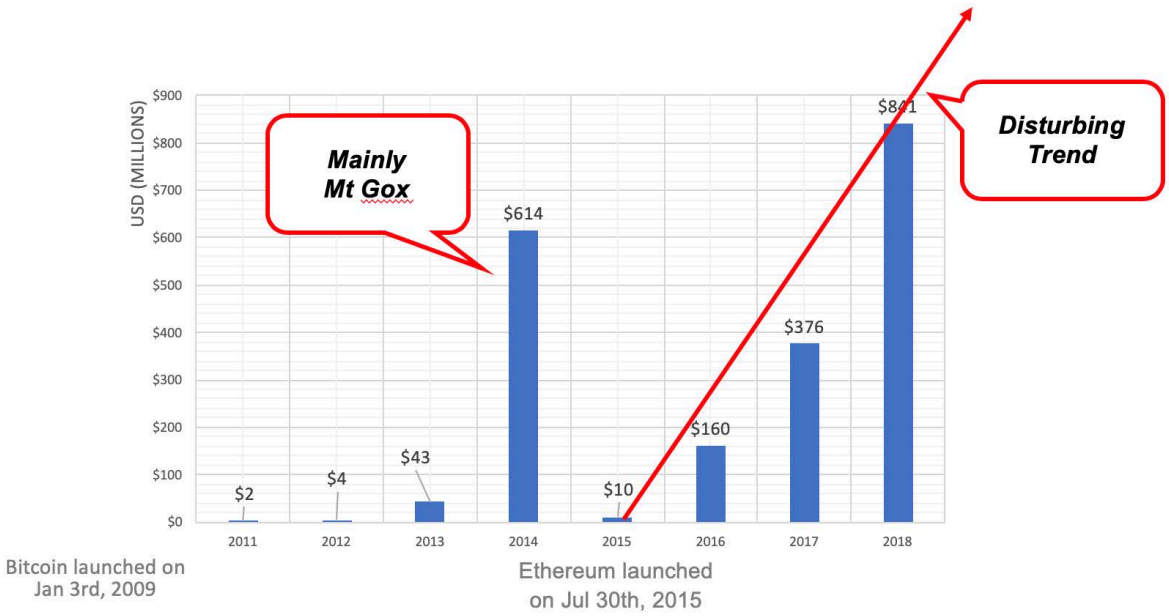


Figure 8. Losses due to cyber security incidents on cryptocurrency exchanges and wallets

Cyber incidents with cryptocurrency exchanges

Research by Chia (2018) reported on the development of a blockchain incident database with approximately 110 incidents collected between 2013 and 2018. Based on an analysis of these incidents, a loss of more than USD 3.5 billion was estimated as a result of cyber incidents on blockchain technology and applications. Adding up all the losses creates a disturbing trend illustrated in Figure 8. While user security like the wide use of two-factor authentication would have tightened as a result of these incidents, cybersecurity measures could become more complex and demanding as they shift to complex technical solutions like cyber defences at the network layers. New IT network level threats can effectively catch up with the less technologically mature crypto-exchanges and would result in incidents or illicit flows.

Blockchain security

While mainly Bitcoin addresses are published in the dark web (Figure 4), the cyber-attacks on cryptocurrency exchanges shows a different distribution based on the blockchain incidents database. Ethereum is clearly number two with a longtail of the altcoins as Figure 9 presents. By analysing the various incidents, it became clear that cyber criminals can enter the exchanges and steal private keys due to poor operational cyber security (OPSEC) measures. In about 66% of cases, OPSEC problems were the cause of the incident. The other major issues were categorized as smart contract security (22%) and issues due to the economic incentives within the blockchain (12%). For the latter category, one can think of stealing energy or to hack for computing power to conduct Bitcoin mining where the benefits end up in criminal wallets. Law enforcement is recommended to build capacity to understand these types of crimes and their underlying causes.

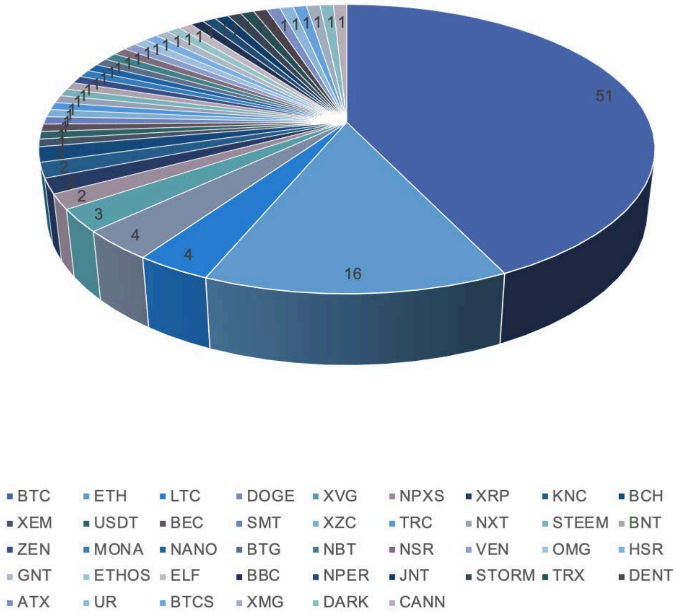


Figure 9. Cryptocurrencies involved in blockchain incidents

Trend 5. Large scale manipulation within blockchain ecosystems

Blockchain ecosystems are distributed and complex systems, so manipulations within these systems are even more opaque and difficult to understand. Two examples will be discussed. First, actors, sometimes called whales, that inject large number of transactions into the markets leading to manipulate virtual asset valuations due to their market domination. Second, centralization of mining pools within the Bitcoin blockchain. The trust in the Bitcoin decentralized ledger relies largely on the fact that the mining system was designed to be distributed to avoid that one entity could manipulate the ledger. If mining pools join forces, this defeats the distribution of control.

Whales

Whales are investors who control more than 1000 Bitcoins.[26] This coin metrics researcher estimates that in December 2019, the whales controlled 42.1% of the total Bitcoin supply. Whether it is fiat, stock exchange or cryptocurrencies, major movements will influence the market. Under this scenario, the strategy to manipulate the valuation is to catch the interest of a critical mass of participants in order to yield a higher (or lower) market capitalization. Those early in the manipulation, the whales, are positioned for maximum profitability. They have visibility and may sell high and buy low for maximum gains. Playing on a rise of the market is called a pump and is a bull market. A fall is a bear market.

According to recent research,[27] it was likely that a single "whale" has manipulated the market and fuelled the Bitcoin valuation hike in 2017. That year, Bitcoin value soared from less than USD 1,000 in January to more than USD 19,000 in December.

---

[26] https://www.latimes.com/business/technology/story/2019-12-12/as-Bitcoin-whales-volatility
[27] Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (October 28, 2019). Available at SSRN: https://ssrn.com/abstract=3195066 or http://dx.doi.org/10.2139/ssrn.3195066

Given the integration of cryptocurrencies into our societies, it is recommended to supervisory bodies, regulators and law enforcement agencies to build capacity to monitor the developments of large-scale manipulations.

Mining pool centralization

Bitcoin mining is carried out by so-called "mining pools", where participating miners compete to be the first to find the next transaction block to add it to the blockchain. In return, the winning miner will receive a reward. The more computing power a mining pool governs, the more likely it could win the competition repeatedly. Recent research[28] has observed centralizing tendencies in these purportedly decentralized mining pools. Statistics, published by blockchain.com confirms this worrying trend and indicate that, as of mid-2019, the overall mining power is concentrated among a relatively small number of pools including BTC.com, ViaBTC and AntPool.

Why is this an issue? The even distribution of mining power (called the hash-rate) is a security parameter for Bitcoin and other cryptocurrencies that rely on mining-based consensus mechanisms. Effectively, one of the threats to the integrity of the blockchain ledger is known as the "51 percent attack". This can occur when an attacker is controlling more than half of the network mining power. The attacker could then subvert the consensus mechanism of the proof-of-work based blockchain, and doing so, could potentially double-spend coins or block transactions. To date, this has effectively occurred 6 times:[29]

- Coilcoin, 6 January 2012
- Feathercoin, 8 June 2013
- Krypton, 26 August 2016
- Verge, 4 April 2018
- Bitcoin Gold, 16 May 2018 (estimated to be the largest loss of all: USD 18 Million)
- Verge, 22 May 2018
- Ethereum Classic, 5 January 2019

While no individual mining pool exceeds or even approaches the 50% limit, large pools could be tempted to hide or disguise the true magnitude of their mining power. Additionally, there is also a risk that two, three or more of the major mining pools join forces and would then easily exceed the critical 50% threshold over extended periods of time.

The mining process is supposed to be a distributed process. However, the current incentives tend to push miners towards a centrally controlled system owned by a small group of actors. This situation requires a close monitoring by law enforcement and requires a coordinated response from the community to design new incentive schemes. This topic is under research

[28] A Deep Dive into Bitcoin Mining Pools – An Empirical Analysis of Mining Shares, 2019; https://arxiv.org/pdf/1905.05999.pdf
[29] https://blog.honeyminer.com/timeline-of-51-attacks/

by the blockchain community.[30] It is recommended to law enforcement to collaborate with this community for security by incentives.

3. Leading regulations and security measures

This paper focuses on an integral analysis of trends and measures for the cyber-enabled component of financial crimes provided by darknet and cryptocurrency ecosystems. The global and foundational regulations against financial crimes are proposed by FATF.[31] The regulation of cryptocurrencies and its participants is a major regulatory challenge. The task force consists of 39 member states to promote and align on international efforts to combat financial crimes. In 2019, FATF published[32,33] its "Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers".

A number of recommendations, regulations, directives and legislations are now in force:

- IMF recommendations;
- UNODC recommendations;
- AMLD5[34];
- Singapore Payment Services Act[35];
- Japan's Payment Services Act and Financial Instruments and Exchange Act[36];
- U.S. Securities and Exchange Commission (US SEC) and Commodity Futures Trading Commission regulatory requirements on cryptocurrency activities.

These efforts are aligned on common goals around anti-money laundering (AML) and Combating Terrorism Financing.

These security measures are completed with existing and leading law enforcement practices[37] and cybersecurity baselines[38] and are addressing the cyber component of financial crimes.

A global approach is fundamental and key, because most cyber-enabled components in financial crimes use the borderless characteristics of cyberspace by involving multiple jurisdictions. To combat these crimes, rules and security measures must be implemented by as many countries as possible, including the financial institutions and VASPs operating from these countries. The challenge is to strike a good balance between the sovereignty of different countries, their legislations, the flexibility to react to local conditions and jurisdictions and, on the other hand, to avoid safe havens for criminals.

---

[30] PREStO: A Systematic Framework for Blockchain Consensus Protocols, Stefanos Leonardos, Daniel Reijsbergen, Georgios Piliouras, IEEE Transactions on Engineering Management, 2019, https://arxiv.org/abs/1906.06540.
[31] FATF Report to the G20 Finance Ministers and Central Bank Governors, July 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf
[32] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html
[33] how do the FATF Standards apply, FATF, http://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets-fatf-standards.html?hf=10&b=0&s=desc(fatf_releasedate)
[34] Strengthened EU rules to prevent money laundering and terrorism financing, June 2018, https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935
[35] Payment Services Act Come Into Force, MAS, January 2020, https://www.mas.gov.sg/news/media-releases/2020/payment-services-act-comes-into-force
[36] Digital Assets in Japan, April 2020, https://innovationlaw.jp/en/digital-assets-in-japan/
[37] https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurrencies
[38] NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

For the national approach to financial crimes, the main thrusts to combat cyber-enabled financial crime are as follows. First, it has been recommended to assign a national authority, in most countries the central bank, to coordinate on the matters of virtual asset regulations. Second, licensing, or at least, registering VASPs. It is important so that perimeter security can be implemented on the exchange between virtual assets and fiat currencies. Third, it is important to establish a Financial Intelligence Unit (FIU). Not all FIUs have enforcement powers and therefore this authority should be equipped with the powers, tools and expertise to liaise between financial institutions and VASPs as well as law enforcement to prosecute financial crimes. This approach should define national governance and facilitate international cooperation, which is essential given the borderless characteristics of cyber-enabled financial crimes.

As a result of the various FATF recommendations, law enforcement approaches and the emergence of VASP industry good practices,[39] the following measures have been identified. These measures have been ranked by the National Institute of Standards and Technology (NIST) cybersecurity framework[40] and ordered by the categories prevent, detect, and respond. These measures are:

(1) Customer Due Diligence (CDD)
(2) Operational Cyber Security (OPSEC)
(3) Intelligence Sharing and Open-source Intelligence (OSINT) Capability
(4) Suspicious Transaction Monitoring and Travel Rule
(5) Intervention on Criminal Infrastructures
(6) Unexplained Wealth Order (UWO) and Virtual Asset Seizure

Measure 1. Customer due diligence (CDD)

This preventive measure introduces real-world identifiers to fight against pseudo-anonymity, remittance, and transaction-based laundering. It would also facilitate traces to potential law and regulation breakers.

FATF recommendation no. 15 (as per date[41]) is most important because it implies that all FATF recommendations[42] are applicable to VAs and VASPs.

According to FATF recommendation n. 10, countries, financial institutes and VASPs should design CDD processes to meet the FATF Standards and national requirements.

---

[39] Project Participate, December 2019, https://www.thecryptoupdates.com/coalition-of-major-stakeholders-in-cryptocurrency-industry-issues-report-on-indicators-of-suspicious-activity/, https://www.forbes.com/sites/michaeldelcastillo/2019/12/04/cryptos-valachi-papers/#631a20903117 or initiatives by V20 and the Global Digital Forum.
[40] https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
[41] Amendment of FATF recommendation 15 in autumn 2018 and the adoption and issuance of an interpretive note to Recommendation no 15 in June 2019.
[42] FATF recommendations and interpretive notes: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

The CDD process should help VASPs in assessing the money laundering and terrorist financing risks associated with covered VA activities, business relationships or occasional transactions above the threshold of 1000 USD/EUR. It is mandatory to do consistent record keeping of transactions for each customer.

CDD process for the VASP comprises of:

(1) Identity check by identifying the customer, also known as KYC during the on-boarding of new clients. Given that identities can be faked, controls are also to be applied on the verification processes of these identities. KYC also establishes the important source of funds/source of wealth and other reference data that is used to check for abnormal transaction characteristics.
(2) For all countries involved, check KYC, AML regulations and enforcement,
(3) Sanctions check, for example, sanctions as published by the Office of Foreign Assets Control.[43] This list mentions special designated nationals including their suspicious cryptocurrency addresses.
(4) AML check on the customer's beneficial owner and verifying the customer's identity on a risk basis and on the basis of reliable and independent information, data, or documentation.
(5) Conduct a politically exposed person (PEP[44]) check.

These checks form the core activities of the financial industry to fight against illicit financial flows. CDD is an important preventive measure, because criminals prefer anonymity in operations and payments, while CDD enforces the opposite. As a result, criminals will move to other VASPs for their operations. CDD would be enforced by the national authorities as part of the licensing process.

Measure 2. Operational cyber security (OPSEC)

This preventive measure is usually imposed by regulatory audits and request for business improvement on VASPs as well as VASPs' own preparations. This measure guards against cyber-attacks.

One of the most common trends in abuse of darknet and cryptocurrencies is trading payment credentials, as was illustrated in Trend 1. These credentials are often stolen during successful cyber-attacks on VASPs, as shown by Trend 4. The right preventive measure is the implementation of good cyber defence by the VASP, as most financial institutions have learned since the 1990s. OPSEC also forms part of incident response playbooks that VASPs should have. Recommended for implementing operational cybersecurity policies are references and guidelines such as the NIST recommendations and the Open Web Application

[43] https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200302.aspx
[44] "PEPs" are individuals who are or have been entrusted with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials (FATF Glossary).

Security Project (OWASP) "top ten".[45] These recommendations should be tailored to each VASPs specific client categories and product activities.

In any case, cyber hygiene must be the starting point to make cyber-attacks less promising and less profitable. Cyber hygiene practices must be implemented and include:

- continuous cybersecurity education of staff,
- awareness of social engineering strategies,
- auditing of hygiene measures,
- and timely reporting of potential incidents.

These practices also include effective in-depth defence and governance structures to drive the implementation of cybersecurity across the whole of the VASP, including third party vendors' interactions with it.

Since OPSEC is not easy to implement and it is known that almost every Internet-connected service is ultimately vulnerable, several layers of OPSEC are recommended. Other non-technical principles must be considered. For example, the four eyes principle[46].

Measure 3. Intelligence sharing and OSINT capability

This detection measure focuses on environment-based information collection from several sources and on its sharing by different stakeholders. This is key to ensure that proper intelligence feeds mechanisms for safeguards and cybersecurity defences.

Usually, the financial institutions and virtual asset service providers base their activities and priorities on sources of information available within their organization. For example, banks use transactional information, and police use criminal databases. Often, relevant and related information is not shared for a variety of reasons including confidentiality, privacy and ethics.

Given that most dark web and VA crimes involve dark markets, signals on activities can be collected since these markets advertise services and goods openly within specific onion services. These signals, including email and cryptocurrency addresses, can be collected via OSINT capabilities. Through this foundation that acts as a constant intelligence feed for horizon scanning, policies can be kept up-to-date to facilitate risk-based approaches to adhere to FATF and other anti-financial crimes. Given the pace of criminal abuse of new technologies, this intelligence gathering should be an institutionalized and continuous process to help timely responses.

Practical tools are available to support OSINT capability like dark web monitoring solutions and blockchain analytics tools as illustrated in Trend 2. Given that this measure is focused on crimes specifically, law enforcement must translate their front-line observations to information products that can serve as input for risk-based approaches by the financial and VASPs.

---

[45] https://owasp.org/www-project-top-ten/
[46] Where the four eyes principle is implemented, decisions require approval from two individuals. This is a deterrent against corruption as well as an effective measure to prevent human errors.

Measure 4. Suspicious transaction monitoring and travel rule

This detection measure seeks to ensure legitimate remittance of transactions, as well as to collect potential evidence against illicit flows.

Suspicious transaction monitoring is one of the most established approaches to combating financial crimes. One of the design criteria for Bitcoin was to develop a monetary system that is independent of financial institutions and other trusted third parties. For this reason, built-in transaction monitoring was not part of this design. On the other hand, the Bitcoin blockchain is a resilient ledger that contains all transactions in a transparent and immutable manner. The main challenge is to attribute these transactions to organizations and natural persons, and to determine in which context a transaction took place to assess suspiciousness.

With the licensing of VASPs, transaction monitoring can be enforced at least on the perimeter between crypto to crypto, and crypto to fiat currencies. According to FATF Recommendation n. 16, which seeks to ensure that basic information can be available to law enforcement agencies to assist them, VASPs have the obligation to obtain, hold, and transmit required information associated with VA transfers higher than 1000 USD/EUR in order to identify and report suspicious transactions. The VASPs should file suspicious transaction reports to the FIU when needed. Second, the FATF recommends that VASPs have to share sender (originator) and receiver (beneficiary) information in cryptocurrency transactions. This is similar to so-called Travel Rules that have for years required financial institutions to share this information when executing bank wire transfers and SWIFT electronic funds transfers essential.

This recommendation is a detection measure that generates needed real-world identifiers. However, criminals are looking for different means to cash out their assets in alternative ways and they spread detection risks by performing multiple smaller transactions, which illustrates one challenge to this security measure. The large number of alternative payment providers created choices for criminals to find the best ways to launder their money.

Measure 5. Intervention on criminal infrastructures

This responsive measure is to conduct law enforcement operations against criminal infrastructures, such as taking down cyber-based illicit services and financial crime activities.

The first large-scale intervention was the takedown of drug-dominated dark market Silk Road 1.0 in 2013.[47] Since then, various interventions have taken place, from suspect arrest, undercover operations, massive takedowns, to the takeover of the Hansa market by the Dutch police in 2017.[48] The first interventions on infrastructures of financial facilitators were reported

[47] https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
[48] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

in 2019. The Dutch Tax Authorities (FIOD) have taken down the first Bitcoin mixing service: bestmixer.io.[49] The importance of this operation lies in the lessons learned about how the mixing service was operated. This helped improve LEA's understanding of the asset trail across mixing services. These operations are always international due to cross-border aspects and as such require international cooperation by law enforcement officers, prosecutors and within the chain of evidence.

Interventions on criminal infrastructures are usually conducted in joint efforts by law enforcement and industry players such as Big Tech[50] and security companies.[51] The preventative value in takedowns or takeovers is the seizure of substantial data, which is used to de-anonymize suspects, estimate transaction volumes, collect investigative leads and even identify potential victims. This information can definitely lead to further police investigations. Second, the preventive effect would discourage other market administrators. But so far, the low risk of being arrested and the potential wealth profits involved limit the deterrent effect. This drawback is illustrated by the fact that a year after the removal of Silk Road 1.0, about 60 new dark markets were counted. This illustrates the displacement effect of this measure and the learning curve of the market administrators. Many of these markets have emerged with improved operational cybersecurity measures, such as encryption in data storage and personal messages.

Measure 6. Unexplained wealth order (UWO) and virtual asset seizure

Finally, this response measure is related to active investigations and acquisition of evidence. The UWO[52] security measure is a court order to compel the target to reveal, block or freeze the sources of their unexplained wealth. The strength of UWOs in AML lies in their reverse onus principle. The suspect must prove his innocence instead of the accuser to prove that someone is guilty.

If cryptocurrencies is a major source of wealth, it is also critical that law enforcement agencies have a good seizure policy. In many countries, law enforcement intervenes in cryptocurrencies, preferably during or just after an arrest. It then sells these fruits of crime as quickly as possible, but without affecting the volatility of the valuation. If the forfeiture turns out to be incorrect, the suspect must reclaim the value in fiat currency when the assets were sold. Currently, several countries have their first cases in this area, which should lead to good practices for seizure directives. INTERPOL Innovation Centre has published law enforcement guidelines for Virtual Asset seizure[53].

These measures are responsive because it takes effect after the crime, when someone has obtained their criminal benefits, and a visible misalignment of lifestyle and formal income

[49] The FIOD and the Public Prosecution Service take money laundering machine for cryptocurrencies offline, 2019, https://www.fiod.nl/the-fiod-and-the-public-prosecution-service-take-money-laundering-machine-for-cryptocurrencies-offline/
[50] https://en.wikipedia.org/wiki/Big_Tech
[51] https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/
[52] https://en.wikipedia.org/wiki/Unexplained_wealth_order
[53] Guidelines for the Seizure and Sale of Virtual Assets, INTERPOL April 2020.

becomes a signal to the investigative authorities. In many cases, the tax administration offices are the first to receive these signals because they are aware of formal income, although it requires combining lifestyle information that is often obtained by law enforcement officers. The strength of this security measure is that it makes crime not beneficial, because the suspect loses all profits.

4. Gap analysis

The previous two sections introduced the five trends in the cyber-enabled components of financial crimes, and the six leading regulatory and security measures. This section analyses the effectiveness of each measure for those trends. This is achieved by a gap analysis that is presented in Table 4.

Table 4. Gap analysis on effectivity of the security measures for the cyber-enabled trends in financial crimes (Y = Yes, N = No, 0 = Neutral)

Security Measures	M1	M2	M3	M4	M5	M6
	Prevent		Detect		Respond	
Trends	Customer Due Diligence	Operational Cyber Security	Intelligence Sharing and OSINT capability	Transaction Monitoring and Travel Rule	Intervention on Criminal Infrastructure	Unexplained wealth order and VA Seizure
T1 Trade in Credentials	Y	Y	Y	Y	Y	Y
T2 Support Illegal Transactions	Y	N	Y	Y	0	Y
T3 Suspicious Cryptocurrency Hubs	Y	N	Y	Y	0	Y
T4 Cyber-attacks on VASPs	N	Y	0	0	N	0
T5 Blockchain Ecosystem Manipulation	0	N	Y	N	N	0

In the above table:

- Green implies the security measure has a real positive impact to reduction the concerned risk
- Orange means the security measure partially influences a reduction of the risk
- Red means no influence on the risk

Trade in credentials of payment methods (T1) can be disrupted by all six security measures. OPSEC and interventions on infrastructures support prevention on the cyber-enabled component of this trend. And the other measures prevent actors to send and receive substantial monetary flows as a result of criminal activities.

To disrupt payment support for illegal transactions (T2), the effective measures are mainly the customer due diligence and transaction monitoring. Information sharing and OSINT should contribute by contextualizing these transactions with proper tags or risk factors. The UWO measure is a last resort.

The security measures to monitor and disrupt activities on suspicious hubs (T3) are only effective when owners of these hubs transfer their funds beyond the crypto perimeter. As long as the funds remain in the crypto-space, only OSINT and Blockchain analytics solutions can be used to identify and contextualize the activities on these hubs.

Cyber-attacks on VASPs (T4) are less effective when proper OPSEC is implemented. The other security measures do not really contribute to this trend, but special attention is required for stolen credentials. In case the VASP reports properly, this information can provide relevant inputs for transaction monitoring by adjusting certain risk factors for specific transactions.

Blockchain ecosystem manipulations (T5) are hard to disrupt, only when these actors are cashing out, it makes these movements visible, and only then can they be attributed to natural persons or organizations. Only possible approach so far is proper monitoring using OSINT and Blockchain analytics tooling, with proper tagging and information sharing.

5. Discussion

The inherent global nature of the VA ecosystem makes VA activities particularly suitable for committing and facilitating transnational crimes. This paper has assessed the effectivity of prevention, detection and response measures, with special attention for the role of law enforcement. This discussion analyses the various observations and puts them into context and operational perspectives, especially with emphasis on, but not limited to, law enforcement.

More complex technology, more complex crimes

The trends show that trade in payment credentials is an established business, while at the same time increasingly complex crimes are committed using the complexity of new technologies and cyberspace. Although many of those crimes are at an early stage, it is essential to identify and monitor these new criminal business models. The sample address with over USD 900 billion in funds received illustrates the complexity of putting the situation into context, as two conflicting explanations have been obtained. Given cryptocurrency addresses that can transmit VAs worth billions of dollars, this should be sufficient reason to improve monitoring at a strategic, tactical and operational level. For example, active hub identification and monitoring requires new roles and capabilities. Most hubs cannot be attributed to a single country, so international cooperation is key. It takes new partnerships and technologies to build capabilities to combat these crimes.

It requires international cooperation and information sharing within and over the stakeholders within governments, finance and law enforcement to build joint strategic pictures about these

crimes. At this stage, criminals could probably see the opportunity faster than the international crime-fighting community can answer.

Effectivity of security measures

The gap analysis shows that the security measures are mainly effective for the more traditional manifestations of cyber-enabled financial crimes. The main challenge here is the need to coordinate a global effort with participation by as many countries as possible to implement these measures. By licensing and registration of VASPs, these policies should be implemented. In case all VASPs are compliant with CDD recommendations, the perimeter is closed and anonymity in cryptocurrencies is nearly impossible. This stage is not yet achieved, but it is definitely the right direction for this preventive measure.

A joint effort by the VASPs and the financial institutes should make it harder for criminal proceeds to be laundered. This is based on the assumption that actors finally want to exit the crypto-space in exchange for fiat currencies. It will take many more years before our societies would support our lives only using cryptocurrencies and no fiat money. However, scenarios where actors cash out amounts below 1000 USD/EUR through different channels on a regular basis are probable and reasonable. In this case, a major part of the VA value remains within the crypto-space. The volatility of the VA valuation is a risk for the VA owners. To influence the volatility are typical scenarios for whales, owners of the suspicious hubs, but also successful vendors in the dark markets.

In most approaches, the combat against the cyber-enabled crimes is focused on the actor and the transactions, and less on the cyber component that facilitates these crimes. This paper gives an integral analysis of this challenge. Cyber-attacks on financial institutes and VASPs have historically been very beneficial for the attackers. So, it is key to impose even more stringent cyber security policies and possibly make cyber security part of the licensing procedure of VASPs. Within different countries, cyber security agencies should provide guidance in order to treat the VASPs similarly to financial institutions that are in most countries qualified as critical infrastructure.

Most security measures are not completely new, but the translation to the new technologies as darknet and cryptocurrencies are far from trivial. The expertise and capacity on these matters are scarce, often because the awareness level is still limited. To implement the security measures, it is eminent that dark web monitoring and blockchain analytics tooling with specific features to combat these cyber-enabled financial crimes are required and should be implemented. For example, solutions are needed to actively translate open source information to inputs for risk-based approaches by the financial institutions and VASPs.

Role and responsibility of law enforcement

Criminals exploit the borderless characteristics of the internet by involving as many jurisdictions as possible in their modus operandi. Most suspects are sufficiently business and tech-savvy to use these opportunities. Thus, cyber-enabled financial crimes have global implications. Capacity building by means of specialized units on darknet and cryptocurrencies

is crucial for law enforcement to be prepared in as many countries as possible. These units should establish the partnerships, expertise and equipment to be effective in this area.

It is in the interest of law enforcement if VASPs and other financial institutions implement proper CDD processes. This information is essential for attribution purposes. Attribution is a particular challenge for cybercrime and cyber-enabled financial crime investigations. Collaboration with cryptocurrency exchanges and other new payment providers with proper KYC implementations is essential, since they can attribute a VA transaction to a natural person or legal entity. Standard operating procedures or SOPs are needed to subpoena these service providers properly. Although not a supervisory body for security measure M1, law enforcement should take the responsibility to report to the national authorities about non-cooperative VASPs, their lack of response and weak implementation of KYC.

It is fundamental that law enforcement officials underline the importance of good OPSEC measures M2 by VASPs, as this strengthens prevention against cyber-attacks. Trend 4 showed VASPs as interesting targets for cyber-attacks. In the event of a successful cyber-attack, law enforcement must be forensically prepared to secure data for investigation and attribution purposes. Cybercrime and digital forensics units should be prepared to conduct forensics on the attacked infrastructures of VASPs for attribution purposes. In many cases, cybercriminals try to steal account details and private keys as valuable VAs. Cyber security agencies should be involved as well to learn from the attacks and when required adjust regulations and defences.

New technologies are needed to equip the specialized units to be able to monitor the dark web and conduct proper cryptocurrency analysis using blockchain analytics tooling to track criminal money-flows. These are basic solutions that support the OSINT capability of security measure M3. It is especially of interest to track transactions from payments supporting illegal transactions and orders to cryptocurrency exchanges. Some blockchain analytics solutions have implemented assets tracking and understanding of the flow with intelligence obtained through crypto-dusting and by sharing TagPacks.[54] TagPacks are a method and format defined by a consortium of partners (including INTERPOL). They enable investigators' sharing of intelligence.

OSINT is key to horizon scanning, especially early warning either expert driven in partnerships or automatically data driven. Many criminals feel safe by using Tor and Bitcoin, so it is well possible they make mistakes in their daily operations, and especially may have made mistakes in the past when not yet familiar with these technologies. That can be used to de-anonymize an actor. It requires the right expertise to identify and exploit these mistakes during the investigations.

Close collaboration with the FIUs is important since they are the core authority receiving and centralizing the STRs/SARs from the obliged reporting entities. This close cooperation is key

[54] https://graphsense.info

for the effectiveness of M4. The INTERPOL Financial Crime Unit is already noticing an increasing trend in the number of reports related to cryptocurrencies and other VAs. This partnership should strengthen the information position and collect leads for investigations.

Several police forces all over the world are conducting darknet and cryptocurrency investigations (M5). As addressed, international collaboration is at the core of these investigations. In many cases, it is rather clear when cryptocurrency addresses can be linked to a crime, and the attribution to the criminal can be done by tracking the cash-out through cryptocurrency exchanges. Possibly more pro-active interventions on criminal infrastructures should be explored by law enforcement as well. Configuration mistakes in criminal infrastructures are already exploited for takedowns. Police shall adapt their covert operating procedures to be able to send small amounts of Bitcoin to suspicious addresses to follow the funds.

Collection of historic information of vendor transactions is also important to estimate the fruits of crime (M6). It requires combining crawled data, seized data (as a result on intervention on criminal infrastructure) and data collected during arrest. Law enforcement agency databases are needed to value cryptocurrencies to the date of transaction. Large-scale calculations should be made based on addresses and transactions attributed to a certain actor to estimate the fruits of crime. Such analytics should include automated identification and analysis of market wallets in order to estimate the size and nature of markets.

6. Recommendations for law enforcement

The observations within this assessment report are driven by the effectiveness of the leading security measures for cyber-enabled financial crimes within the era of darknet and cryptocurrencies. Achieving this high-level goal, based on the analysis in this assessment report, requires global efforts to emphasize the implementation of the addressed security measures. Specifically for law enforcement, this results in the following recommendations.

Recommendation 1. Focus on prevention, detection and response policies

Implementation of these policies is key to disrupt cyber-enabled financial crimes. As addressed by the discussion on the law enforcement role, law enforcement has a leading or supportive role on each security measure. To implement those is not trivial, it requires new partnerships, new expertise and new tooling that needs to be incorporated within the police forces.

Given the natural focus of law enforcement on crime, law enforcement should lead and share strategic insights about innovations in the area of cyber-enabled financial crimes with all relevant stakeholders. It requires continuous horizon scanning as an essential activity to provide insights on size and nature, changes in modus operandi and new criminal business

models as inputs for assessments by the community to evaluate whether the security measures are still effective. The strategic and tactical insights need to be shared with partners such as financial institutions or cybersecurity agencies to help them adjust their priorities. In other words, the strategic information shared by law enforcement should serve as inputs for the risk-based approaches that financial institutions and security actors use to enrich their protective measures.

Recommendation 2. Focus on innovation and technology

New law enforcement capabilities are needed to tackle the crimes as identified by the five trends. Many countries have established specialized units that focus on darknet and cryptocurrencies. These units need tools to support on a strategic, tactical and operational level. Technical attribution of the digital traces is an essential law enforcement capability that requires support with innovation and technology.

Dark web crawling and blockchain analysis tools are basic technologies every law enforcement agency in the world needs to combat cyber-enabled financial crimes. These solutions should map criminal activities on service categories, abuse types and geographic locations to improve attribution [Spitters 2015] to natural persons and organizations. Standard taxonomies are required to establish a common language for horizon scanning and international cooperation. This common language for categorizing and analysing these crimes is essential for a global understanding.

Recommendation 3. Focus on international collaborative mechanisms

Cyber-enabled financial crimes, like most cybercrimes, are not limited to individual jurisdictions and intentionally use the borderless characteristics of cyberspace to complicate prosecution. It is essential to develop those mechanisms of cooperation within the international public-private community to act quickly and effectively against crimes. While law enforcement is one of the stakeholders in this community, it is crucial to actively contribute to the multi-stakeholder global efforts.

Developing effective international collaborative mechanisms is a joint responsibility where organizations such as INTERPOL can lead international efforts. Building joint strategic insights on criminal activities in different countries is an essential starting point to set priorities. In addition, it is important to develop principles of information sharing so that key partners are well informed and able to contribute through their role and responsibility. For example, the INTERPOL Working Group on Darknet and Cryptocurrencies is an important platform where latest trends and good practices are shared among member countries, including contributions from private sector and academia.

7. Acknowledgement

This paper was prepared for the INTERPOL Innovation Centre by:

- Prof. Lam Kwok Yan (School of Computer Science and Engineering, and Director of the Nanyang Technopreneurship Center, Nanyang Technological University (NTU), Singapore)
- Boon-Hiong Chan (M.Sc in Computation (Artificial Intelligence)), **GIAC** Security Essentials Certification
- Prof. Emeritus Pieter Hartel (CFLW Cyber Strategies, Principal Cyber Security and Privacy, The Netherlands)
- Dr. Mark van Staalduinen (Director of CFLW Cyber Strategies, and specialist consultant to the INTERPOL Cyberspace and New Technologies Lab in Singapore)

Finally, we would like to thank our contributors for peer reviewing of this document, and for greatly assisting in providing additional insights and trends and to ensure alignment with law enforcement practices:
Priscilla Cabuyao, Vincent Danjean, Sinyoung Kim, Luciano Kuppens, Shun Inagaki, Sandi Pirc and Alexander Resch.

8. Key references

[Caneppele 2019] Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes; Stefano Caneppele, Marcelo F Aebi; Policing: A Journal of Policy and Practice, Volume 13, Issue 1, March 2019, Pages 66–79, https://doi.org/10.1093/police/pax055, 13 September 2017

[Chia 2018] Vincent Chia, Pieter Hartel, Qingze Hum, Sebastian Ma, Georgios Piliouras, Daniel Reijsbergen, Mark van Staalduinen, and Pawel Szalachowski. Rethinking blockchain security: Position paper. In Mohammed Atiquzzaman, Jin Li, and Weizhi Meng, editors, Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, pages 1273-1280, Halifax, Canada, Jul 2018. IEEE. Topic-Review. URL: https://doi.org/10.1109/Cybermatics_2018.2018.00222.

[Fanusie 2018] Y. J. Fanusie and T. Robinson. Bitcoin laundering: An analysis of illicit flows into digital currency services, Jan. 2018. A memorandum by the Center on Sanctions and Illicit Finance and Elliptic.

[Spitters 2015] Martijn Spitters, Femke Klaver, Gijs Koot, and Mark van Staalduinen. Authorship analysis on dark marketplace forums. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Manchester, UK., Sep 2015. IEEE. Topic-Horizon-Scan.

9. Acronyms

2FA – two factor authentication
AEC – Anonymity enhanced cryptocurrency
AML – Anti-money laundering
AMLD5 – Fifth European anti-money laundering directive
CCD – Customer due diligence
CNTL –cyberspace and new technologies laboratory (INTERPOL innovation centre,)
CTF – Combating terrorism financing
CTFC – US commodity futures trading commission
DDoS – Distributed denial of service attacks
DWM – Dark Web Monitor
EU – European Union
EUR – Euros
FATF – Financial action task force
FIOD - Fiscale Inlichtingen en OpsporingsDienst (Fiscal Information and Investigation Service)
FIU – Financial intelligence (or investigation) Unit
GIAC – Global information assurance certification
HTML – Hypertext markup language
IC - INTERPOL innovation centre
IEEE – Institute of electrical and electronic engineering
IMF – International monetary fund
IT – Information technology
JCB – Japan credit bureau
KYC – Know your customer
LE and LEA – Law enforcement agency
NGO – Non-governmental organization
NIST – National institute of standards and technology
OFAC – US Office of foreign assets control
OPSEC – Operational cyber security
OSINT – Open source intelligence
OWASP – Open web application security project
PEP – Politically exposed person
SOP – Standard operating procedure
STR – Suspicious transaction report
SWIFT - Society for worldwide interbank financial telecommunication
UNODC – United nations organization office on drugs and crime
USD – United States dollars
USSEC – US securities and exchange commission
UWO – Unexplained wealth order
VA – Virtual Asset
VASP – Virtual asset service provider

10. Cryptocurrency coins and tokens mentioned

ATX – Aston token or Artex coin
BAT – Basic attention token
BBC – Bitconnect cryptocurrency token, defunct
BCH – Bitcoin cash
BEC – Beauty chain crypto token
BNB – Binance coin (Binance.com)
BNT – Bancor coin
BTC – Bitcoin
BTCS – Bitcoin scrypt coin
BTG – Bitcoin gold coin
CANN – Cannabis coin
CRO – Crypto.com coin, same as MCO
DAI – Dai stablecoin
DARK – DarkCoin
DENT – Dentcoin token (Dent telco)
DOGE – Dogecoin
ELF – Aelf token
ETH – Ethereum
ETHOS – Ethos coin
GNO – Gnosis coin
GNT – Golem network token
GUSD – Gemini dollar stablecoin
HSR – Hshare coin
HT – Huobi token (Huobi.com)
JNT – Jibrel network token
KNC – Kyber network token
LEO – Leo coin (Bitfinex.com)
LINK – Chainlink token (Line corporation, Japan)
LTC – Litecoin
MCO – Crypto.com token, same as CRO
MKR – Maker Token (MakerDAO, decentralized autonomous organization)
MLN – Melon token
MONA – MonaCoin
NANO – Nano coin (formerly XRB – Railblocks)
NBT – NuBits, NiceBytes or Ninsa B token
NPER – Decentralized intellectual property network token
NPXS – PundiX token
NSR – NuShares token
NXT – nxt coint (BCNext, now Jelurida SA)
OMG – OmiseGo token

PAX – Paxos standard stablecoin (Paxos trust company LLC)
SMT – Smart mesh token
STEEM – Stem power coin (Steemit Inc)
STORM – Storm token
TRC – Terracoin
TRX –Tronix coin, or Tron
TUSD – TrueUSD stablecoin (TrueCoin LLC)
UR – UR coin, defunct
USDC – USD Coin stablecoin (Circle.com and Coinbase.com)
USDT – Tether stablecoin (Tether Ltd)
VEN – VeChain token
WETH – Wrapped ETH token
XEM – New economy movement coins
XMG – Magi coin
XRP – Ripple coin
XVG – Verge coin
XZC – Zcoin token
ZEN – Horizen token (Horizen Labs)
ZIL – Zilliqa coin
ZRZ – ZRZ token, defunct

INTERPOL

ABOUT INTERPOL

INTERPOL's role is to enable police in our 194 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support three global programmes: counter-terrorism, cybercrime, and organized and emerging crime.

WWW.INTERPOL.INT